FORTINET
High Performance Network Security

Customer Data Handling for Fortinet Services and Websites

Version 1.0

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FORTINET PRIVACY POLICY

https://www.fortinet.com/corporate/about-us/privacy.html

FEEDBACK

Email: techdocs@fortinet.com

6 December 2017

Customer Data Handling for Fortinet Services and Websites

Version 1.0

01-100-447922-20171206

TABLE OF CONTENTS

Change Log **4**
Introduction **5**
Terms of Service 5
FortiGuard 5
FortiCare 5
FortiCloud 6
FortiCloud Sandbox 6
FortiMail Cloud 6
Privacy Practices specific to Fortinet Services **7**
Information collected by Fortinet Services 7
Uses of information collected by Fortinet Services 8
How customer information is stored and protected 10
Data retention 11
Privacy Practices specific to Fortinet Websites **12**
Information collected through the Fortinet Websites 12
Information you provide to us through the Fortinet Websites 12
Information collected automatically through the Fortinet Websites 12
Use of your information collected through the Fortinet Websites 14
Additional information about our Privacy Practices **15**
Information from Third Parties 15
Aggregated or De-Identified Data 15
Sharing of Your information 15
Your Email Marketing Choices 15
Third Party Links and Services 16
Security of Your Personal information 16
Additional Details About Your Personal information Rights 16
International Data Transfer 16
Your California Privacy Rights 17
Notification of Changes 17
Contact information **18**

Change Log

Date	Change Description
6 December, 2017	Initial release.

Introduction

This document describes how customer information and data is treated in terms of security and privacy by Fortinet, Inc. and its wholly-owned subsidiaries and affiliates (collectively, “Fortinet”, “we”, “our”, or “us”). We provide security solutions that protect networks, users, and data from continually evolving threats.

The types of customer information and data involved includes:

- Information we receive through our products, support, or cloud-based services (collectively, the “Fortinet Services”), including:
  - FortiGuard
  - FortiCare (Fortinet's Support site)
  - FortiCloud (logs and management)
  - FortiCloud Sandbox (also known as FortSandbox Cloud)
  - FortiMail Cloud
- Information we receive through our website at www.fortinet.com or any other Fortinet website on which this Policy is posted (“Fortinet Websites”).

This document is based on Fortinet's privacy policy (https://www.fortinet.com/corporate/about-us/privacy.html) and also includes more details about privacy practices specific to Fortinet services.

Terms of Service

A current description of the Terms of Service for Fortinet Services can be found at: https://www.fortinet.com/content/dam/fortinet/assets/legal/Fortinet-Service-Offering-Terms.pdf

Fortinet services discussed in this document do not share or make available any data to any third-parties.

FortiGuard

FortiGuard is Fortinet's threat research and protection service. Fortinet's FortiGuard threat research team discovers and studies breaking threats and updates FortiGuard security services to protect Fortinet's customers against those threats. For more information, see:

- http://fortiguard.com

FortiCare

FortiCare provides Technical Support Services for registered Fortinet customers. For more information, see:

- http://support.fortinet.com

FortiCloud

FortiCloud provides centralized reporting, traffic analysis, configuration management, WiFi management, and log retention for Fortinet's products without the need for additional hardware, software or management overhead. For more information see:

- http://forticloud.com
- https://docs.fortinet.com/uploaded/files/3769/forticloud-service-description.pdf

FortiCloud Sandbox

FortiCloud Sandbox is a proactive threat detection, mitigation and actionable threat insight solution. At its foundation is a, dual-level sandboxing platform that is complemented by Fortinet’s antimalware and integrated FortiGuard threat intelligence.The FortiCloud Sandbox Service allows the customer to deploy Sandboxing in a flexible, distributed architecture. For more information, see:

- https://docs.fortinet.com/uploaded/files/3429/FortiSandbox-Cloud-Service-Description.pdf

FortiMail Cloud

FortiMail Cloud Email Security is Fortinet's secure cloud email gateway solution. Fully managed by Fortinet, FortiMail Cloud is available in 2 different deployment options:

- **Gateway**, route email to Fortinet where it is cleaned of malware and spam and forwarded onwards to existing customer mail servers.
- **Server**, hosted email infrastructure and security with Fortinet Malware and spam protection as well as protection of sensitive information.

For both deployments FortiMail Cloud there is a Premium option, which adds Data Loss Prevention, Identity Based Encryption and Sandboxing. For the Server offering, the Premium service also adds additional mailbox storage. For more information, see:

- https://docs.fortinet.com/uploaded/files/3303/FortiMail%20Cloud_Service_Description.pdf

Privacy Practices specific to Fortinet Services

This section includes the privacy practices and policies for Fortinet Services.

Information collected by Fortinet Services

Through the following Fortinet Services, we may collect or process (sometimes just momentarily) a variety of information about users of the Fortinet Services, associated devices, and networks connected with the Fortinet Services, including:

FortiGuard

Most registered Fortinet products send some or all of the following information to FortiGuard:

1. Product serial number and IP address used for requesting FortiGuard updates.
2. Firmware version and information about FortiGuard updates.
3. Email address used for logging into the Fortinet Support website and registering the Fortinet product.
4. Virus statistics (if the product supports virus scanning).
5. URLs submitted for URL ratings (if the product supports FortiGuard web filtering).
6. AntiVirus, IPS, and Application Control Malware statistics.

FortiClient sends the following information to FortiGuard:

1. OS information (version and hardware information, including CPU and RAM, time zone, and language).
2. FortiClient version information and features.
3. Virus statistics.
4. URLs submitted for URL ratings.

FortiGuard website

Any Internet user can interact with Fortinet through the FortiGuard website at http://www.fortiguard.com to submit a suspicious file for scanning, appeal a blacklisted address or URL, dispute a software classification, report a virus, submit a general question, and so on. To submit a query or request, the user must include an email address. No other personal information is required and the user is not required to log in.

FortiCare

FortiCare customer data is used for customer service, technical support, contract renewal, product registration, license, and service contract activation and the return merchandise authorization (RMA) process. The following FortiCare related information is collected:

1. Customer name, email address, phone number, physical address, device location, serial numbers, and contract numbers.
2. Customer tickets, may include the following information:
   - Description of customer's problem.
   - Network topology diagram.

- Fortinet product configuration.
- Fortinet product logs.
- Packet capture files (traffic content).
- Suspicious files.

FortiCloud (Logs and Management)

Fortinet's customers can use the free or paid FortiCloud service to save logs, reports and configuration files to FortiCloud. Logs and reports can include:

- Device identifiers, IP addresses, and other information about computing systems, applications, and networks.
- Information about activity on computing systems, applications, and networks.
- Communication metadata.
- Suspicious files sent out by the Fortinet product.

FortiCloud Sandbox

If FortiCloud Sandbox is enabled, Fortinet products can send the following data to FortiCloud Sandbox:

- Device identifiers and IP addresses.
- Suspicious URLs submitted for analysis of web contents.
- Suspicious files, communication content, and metadata.

FortiMail Cloud

FortiMail Cloud stores the following customer data.

In Gateway mode

- Sender and receiver email addresses and email subjects, email content is **not** stored.
- Quarantined files.

In Server mode

- Email addresses.
- Aliases.
- Distribution lists.
- Email message content, including attachments.
- Quarantined files.

Uses of information collected by Fortinet Services

Subject to applicable contractual and legal restrictions, and depending on the particular Fortinet Services at issue, we use and disclose the information, as described in this document for the following purposes:

- To improve Fortinet Services by:
  - Providing analysis, maintenance, and technical support.

  - Providing product upgrades.
  - Managing and renewing subscriptions.
- To enforce the legal terms that govern Fortinet Services.
- To comply with law and protect rights and property.
- For other purposes requested or authorized by our users.

Various Fortinet Services use automated technology to recognize and defend against security threats, such as by blocking or quarantining suspected malicious data. In addition, to improve security, Fortinet may exchange certain threat indicators, such as virus signatures or techniques for detection of malicious activity, with other security organizations.

Certain Fortinet Services make certain information they collect available to the customer that manages the service. This customer could be a service provider managing a Fortinet product and the service provider would then have information from Fortinet about the service provider's customers. Customers of the service provider should contact the service provider for details.

We conduct the above activities on the basis of our legitimate interests in operating our business and protecting our customers. Where appropriate, these activities also are conducted on the basis of consent.

The following sections describe the information collected by specific Fortinet Services and what that information is used for:

FortiGuard

- **Unrated URLs:** (URLs that have not been rated by FortiGuard.) Information about the URL, including the FQDN and IP address, is gathered to prioritize adding the URL to FortiGuard for service improvement.
- **Virus statistics:** Fortinet's AntiVirus team calculates statistics on virus infection for service improvement.
- **Fortinet product serial number:** For contract management.
- **Fortinet product IP address:** To push FortiGuard updates and embargo country controls.
- **Email addresses from FortiGuard website queries**: Sent to an internal email server and used for replying to queries.

Submission of Malware statistics to FortiGuard

Some Fortinet products periodically send encrypted AntiVirus, IPS, and Application Control Malware statistics to FortiGuard. Malware statistics are accumulated and sent periodically (by default every 60 minutes). Included with these Malware statistics is the IP address and serial number of the Fortinet product, and the country in which the Fortinet product is located. The statistics are used to improve various aspects of Malware protection.

For example, AntiVirus statistics allow FortiGuard to determine which viruses are active in the wild. Signatures for such viruses are kept in the Active AV Signature Database that is used by all Fortinet products. Signatures for inactive viruses are moved to the Extended/Extreme AV Signature Database. If the events involving inactive viruses start appearing in Malware statistics, these signatures can be moved back to the Active AV Signature Database.

Communication between Fortinet products and FortiGuard servers use 2-way SSL/TLS 1.2 authentication before any data is transmitted. The certificates used in this process must be trusted by each the Fortinet product and FortiGuard and signed by Fortinet CA server.

Fortinet products can only accept data from authorized FortiGuard severs. The server list is updated periodically through previously connected servers. DNS is used by the Fortinet product to find a FortiGuard server. All other servers are provided by a list that is updated through the encrypted channel.

All Malware statistics collected by FortiGuard are used to improve the performance of Fortinet products and services and to display statistics on Fortinet's Support site for customers who registered the Fortinet product.

Statistics or results derived from this Malware data may also be published or shared with various audiences as we deem appropriate. The Malware statistics shared in this way do not include any customer data.

FortiCare

FortiCare data is used for customer service, technical support, contract renewal, product registration, license, and service contract activation and the return merchandise authorization (RMA) process.

- For registration, customer information is passed to Fortinet's customer database service for customer screening.
- For online renewals, customer credit card transactions are passed to a third-party secure credit card processing service. Credit card information is not stored by FortiCare.
- In EMEA, some of Fortinet's distributors handle FortiCare tickets for their customers. These distributors have access to customer tickets related to Fortinet products sold by that distributor.

FortiCloud (Logs and Management)

- Logs are used for FortiCloud report generation.
- All analysis and generation of reports is performed within FortiCloud servers.
- Deletion and retention of configuration files is managed by customers .

FortiCloud Sandbox

- If files are determined to be malicious, the file's checksum is stored by FortiCloud Sandbox.
- If URLs are determined to be malicious, the URLs are stored by FortiCloud Sandbox.

FortiMail Cloud

- Files determined to be suspicious are sent to FortiCloud Sandbox.
- URLs are analyzed. Any malicious URLs will be sent to and stored by FortiCloud Sandbox.

How customer information is stored and protected

For all Fortinet services, including FortiGuard, FortiCare, FortiCloud, FortiCloud Sandbox and FortiMail Cloud the following protection measure are used. These measures follow industry best practices, ISO 27001, and NIST 800-53 guidelines.

- Physical and environmental policies (all Fortinet servers and located in secure Fortinet data centers).
- System administration plans.
- Information security policies.
- Secure communication with third parties.

Data retention

Certain data is only stored for a finite period of time across Fortinet Services, according to service term agreements and the necessity for log analysis.

FortiGuard

- URLs are stored for 2 years.
- Virus statistics are stored for 6 months.
- Fortinet product serial numbers, contract management, IP address, and information about FortiGuard updates are not deleted.

FortiCare

- FortiCare customer data is not deleted.

FortiCloud (Logs, reports and configuration files)

- The paid FortiCloud service retains log and report data for 1 - 5 years depending on the terms of the contract.
- The free FortiCloud service retains log and report data for 7 days or up to a maximum of 200,000 logs.
- If a customer's paid FortiCloud contract is terminated or expires, log retention reverts to the free plan (log and report data is kept for 7 days or up to a maximum of 200,000 logs).
- For all FortiCloud plans (free or paid) saved configurations are never deleted by FortiCloud. Customers can delete them as required.

FortiCloud Sandbox

- If a file or URL cannot be scanned within a 2 hour period, it will be removed from the submission queue.
- All clean files are deleted within 72 hours. All malicious or suspicious files are kept for a maximum of 60 days
- URLs are stored for 2 years.
- Logging of malicious or suspicious activity is stored for 1 year.
- Suspicious files are deleted 2 hours after they are received.

FortiMail Cloud

- In Gateway mode, customers can configure how long email traffic logs are stored.
- In Server mode, customers can configure how long email messages are stored.
- FortiMail VM images are retained for up to 30 days deleted immediately by customers.

Privacy Practices specific to Fortinet Websites

This section includes the privacy practices and policies regarding how data is collected, which information is provided to us by you, and information that is automatically collected.

Information collected through the Fortinet Websites

When you use the Fortinet Websites, we may collect information when you provide information directly to us and when we passively collect information from you.

Information you provide to us through the Fortinet Websites

Information you may provide to us may include (without limitation): your name, address, phone number, email address, credit card number, or other payment details. For example, we collect this information when you fill out an online form, contact us for information or customer support, register to use a service, make a purchase, and request certain features (e.g., newsletters, updates, and other products or services).

In order to tailor our communications to you and continuously improve our products and services (including registration), we may also ask you to provide us with information regarding your personal or professional interests, experience with our products, and more detailed contact preferences. Please note that you always have the option of not providing us this information.

We may enable you to send communications to us or to third parties, such as through our live chat feature. All such communications become our property once you submit them. Without limiting the foregoing, when you provide us with suggestions or feedback for any of our products and services, you grant us an irrevocable, exclusive, royalty-free, perpetual, worldwide license to use, modify, prepare derivative works, publish, distribute and sublicense the suggestions or feedback. When you choose to initiate communication with us, or anyone else, you may be contacted in return. Please use your discretion when deciding whether and what to communicate.

We reserve the right, in our sole discretion, to monitor, edit or delete communications transmitted to us or that are made publicly available on the Fortinet Websites, but we have no obligation to do so, and we will not be liable for any such edits or deletions.

Information collected automatically through the Fortinet Websites

We may automatically collect information about how you access and use the Fortinet Websites. For example, we may collect and store information such as your browser type, IP address, language, operating system, the state or country from which you accessed the Fortinet Websites, the pages you view, the services you use, the date and time of your visit, the websites you visited immediately before and after visiting our websites, error logs, and other hardware and software information.

Fortinet may maintain logs of the traffic that visits the Fortinet Websites. Log files are used to manage traffic loads and information technology requirements for providing reliable service and for other purposes. We may use third party analytics providers, such as Google Analytics, and various technologies, including cookies and similar tools, to assist in collecting this information. We may use this information to formulate statistical models about use of the Fortinet Websites, enhance the Fortinet Websites for our users, and provide you with tailored content and advertising.

To prevent Google Analytics from using your information in a particular browser for analytics, you may install the Google Analytics Opt-Out Browser Add-on by clicking here.

Cookies

The Fortinet Websites may use cookie technology and similar online tools, such as web beacons and web pixels. “Cookies” are small files that a website stores on a user’s computer or device. We use cookies to identify customers when they visit our sites. Cookies are used to remember user preferences and maximize performance of the Fortinet Websites. Additionally, cookies help us to identify returning users so that we don't ask them to enter their email and password with every visit.

Most web browsers automatically accept cookies, but you may set your browser to block cookies (consult the instructions for your particular browser on how to do this). Please note that if you decide to block cookies, this may interfere with your ability to perform certain transactions, use certain functionality, and access certain content on the Fortinet Websites.

Tailored Advertising

The Fortinet Websites may include third party cookies and other advertisement technology that enables customized ads to be displayed to you through the Fortinet Websites and elsewhere online. When you use the Fortinet Websites, we or third parties operating the ad serving technology may use device or similar information that is collected through cookies, web beacons, pixels, clear GIFs, or similar technologies to customize ads and to perform analytics concerning your use of the Fortinet Websites and other websites tracked by these third parties. These technologies may also control the number of times you see a given ad, deliver ads that relate to your interests, and measure the effectiveness of ad campaigns.

To the extent any of this information is collected by third parties, you acknowledge and agree that such collection and use is governed by those third parties’ privacy policies and we are not responsible for the privacy practices of such third parties. Cookies may be associated with de-identified data linked to or derived from data you voluntarily have submitted to us (e.g., your email address) that we may share with a service provider in hashed, non-human readable form.

For more information about tailored ads and your choices to prevent some of these third parties from delivering tailored ads, you may visit the following third party websites:

- Network Advertising Initiative Consumer Opt-Out Page
- Digital Advertising Alliance’s Consumer Opt-Out Page

You can also visit the Google Ad Settings page to adjust your preferences regarding certain ads facilitated by Google.

Please note that you will still receive ads even if you opt out of tailored ads. In that case, the ads will just not be tailored to your interests. If your browser is configured to reject cookies when you visit an opt-out page, or you subsequently erase your cookies, use a different computer or change web browsers, or your opt-out may no longer be effective. Also, the opt-out services identified above are controlled by those third parties, not Fortinet, and Fortinet does not control which companies choose to participate in those programs.

Do Not Track

We are committed to providing you with meaningful choices about the information collected on our Services for third party purposes, and that is why we provide the various advertising opt outs above. However, we do not recognize or respond to browser-initiated Do Not Track signals, as the Internet industry is still working on Do Not Track standards, implementations, and solutions.

Use of your information collected through the Fortinet Websites

Fortinet uses and discloses information collected though the Fortinet Websites to better understand your needs and provide better service. We may use the information to:

- Process and respond to your inquiries
- Help you complete a transaction, including fulfillment of orders and promotional offers
- Manage and renew your subscription(s)
- Send you marketing or other communications that may be of interest to you
- Update you on service and benefits
- Analyze the accuracy, effectiveness, usability, or popularity of the Fortinet Websites
- Improve the content and features of the Fortinet Websites, Fortinet Services, or develop new products and services
- Administer and troubleshoot the Fortinet Websites
- Enforce the legal terms that govern the Fortinet Websites
- Comply with law and protect rights and property
- Fulfill other purposes requested or authorized by our users

We conduct those activities either on the basis of our legitimate interests in operating our business or on the basis of consent.

Additional information about our Privacy Practices

The following additional information is applicable to both Fortinet Services and Fortinet Websites.

Information from Third Parties

We may obtain additional information about you from third parties such as marketers, partners, researchers, and others. We may combine information that we collect from or about you with information we obtain about you from such third parties and affiliates, and information derived from any other subscription, product, or service we provide.

Aggregated or De-Identified Data

We may aggregate and/or de-identify information collected by the Fortinet Websites or Fortinet Services or via other means so that the information does not identify you. Our use and disclosure of aggregated, anonymized, and other non-personal information is not subject to any restrictions under this Privacy Policy, and we may disclose it to others without limitation for any purpose.

Sharing of Your information

We may share your information in the following ways:

- We may share information with other companies and individuals that assist us
- We may access or disclose information about you, including the content of your communications, when we believe in good faith that such disclosure is necessary and appropriate in order to:
    a. comply with the law or respond to lawful requests or legal processes,
    b. protect the rights or property of Fortinet or our partners or customers, including the enforcement of our agreements or policies, or
    c. protect the personal safety of individuals such as Fortinet employees, partners, customers or the public
- We may share your information with any affiliate or agent of Fortinet in order to provide the Services or perform services on our behalf
- We may also disclose, sell or assign personal information in connection with or in anticipation of a corporate transaction, such as a merger, acquisition, sale of assets or restructuring
- We may also share your information when we have appropriate consent or when otherwise permitted by law

Your Email Marketing Choices

If you provide us with your email address, we may occasionally send you emails with recommendations or notices regarding our products, prices, and services. This email may include paid advertisements from third parties. We

will include unsubscribe instructions with such commercial communications. Please note that these opt-out processes may take some time to complete, consistent with applicable law.

Separately, we send service notifications via email to keep you informationrmed about the status of your service orders or accounts and to provide updates and technical notices. These messages are informational and essential to the maintenance of your subscription and the functionality of our services. There is thus no opt-out for service notifications.

Third Party Links and Services

The Fortinet Services and Fortinet Websites may contain links to third-party websites, including social networking websites. Your use of these features may result in the collection or sharing of information about you, depending on the feature. Please be aware that we are not responsible for the content or privacy practices of other websites or services to which we link. We do not endorse or make any representations about third-party websites or services. The personal information you choose to provide to or that is collected by these third parties is not covered by our Privacy Policy. We strongly encourage you to read such third parties' privacy policies.

Security of Your Personal information

We have put in place physical, electronic, and managerial procedures to safeguard data and help prevent unauthorized access, to maintain data security, and to use correctly the data we collect. However, we cannot assure you that data that we collect will never be disclosed in a manner that is inconsistent with this Privacy Policy.

If a password is used to help protect your personal information, it is your responsibility to keep the password confidential. Do not share this information with anyone.

Additional Details About Your Personal information Rights

You may review and update certain user information by logging in to the relevant portions of the Fortinet Services or Fortinet Websites where such information may be updated. In addition, the law of your jurisdiction may give you the right to request access to and rectification or erasure of certain personal data we hold. It may also give you the right to request restrictions on the processing of your personal data, or to withdraw consent for the processing of your personal data. You may contact us as described below to make these requests.

In situations in which we process your personal data only on behalf of our customer (typically the case with respect to our processing of personal data collected through the Fortinet Services), we may refer your request to the relevant customer and cooperate with their handling of the request. You may contact us with any concern or complaint regarding our privacy practices, and you also may lodge a complaint with the relevant governmental authority.

International Data Transfer

The data centers that hold data collected by FortiCloud Services (FortiCloud, FortiCloud Sandbox, and FortiMail Cloud) are located in the European Union and in Canada (on the basis of the European Commission's decision 2002/2/EC, which recognizes that the Canadian Personal information Protection and Electronic Documents Act provides adequate data protection). This data is not hosted in the United States.

Certain commercial data, such as customer records and including the name, phone number and email address of our main contact at each customer, that is collected by other Fortinet services (including FortiGuard and FortiCare) may be stored in the United States or elsewhere outside your country.

Your California Privacy Rights

Subject to certain limitations, California law permits California residents to request and obtain from us a list of the third parties to whom we have disclosed personal information (if any) for the recipient's direct marketing purposes in the prior calendar year, as well as the type of personal information disclosed to those parties. If you are a California resident and would like to request this information, please submit your request in an email to privacy@fortinet.com.

Notification of Changes

Fortinet reserves the right to change this Privacy Policy at any time to reflect changes in the law, our data collection and use practices, the features of our services, or advances in technology. Please check this page periodically for changes. Your continued use of the services following the posting of changes to this policy will mean you accept those changes.

Contact information

If you have questions regarding our practices and Privacy Policy, please contact us at privacy@fortinet.com.